BY ORDER OF THE COMMANDER
AIR FORCE SPACE COMMAND

AIR FORCE SPACE COMMAND INSPECTION CHECKLIST 31-0013

1 OCTOBER 1999

Security

INFORMATION SECURITY (WING)

OPR: SFOP (MSgt Thor Hansen)

Certified by: SFO (Lt Col Clifford E. Day)
Pages: 10
Distribution: F

This Checklist reflects Command requirements for Information Security offices to prepare for and conduct internal reviews.

1. References have been provided for each item. Critical items have been kept to a minimum and are related to public law, safety, security, fiscal responsibility, and/or mission accomplishment. While compliance with non-critical items is not rated, these items help gauge the effectiveness/efficiency of the function.

2. This publication establishes a baseline checklist. The checklist will also be used by the Command IG during applicable assessments. Use the checklist at **Attachment 1** as a guide only. Add to or modify each area as needed, to ensure an effective and thorough review of the unit Information Security Program.

JAMES M. SHAMESS, Colonel, USAF
Director of Security Forces

Attachment 1

INFORMATION SECURITY (WING)

Table A1.1. Checklist.

MISSION STATEMENT: To ensure effective management of the Air Force Information Security program. ***NOTE:*** All references are from DoD 5200.1-R, Jan 1997, unless otherwise stated.			
SECTION 1: DECLASSIFICATION AND DOWNGRADING			
1.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
1.1.1. Does the Information Security Program Manager (ISPM) ensure requests to declassify and release information are reviewed by an original classification authority (OCA)? (para 2-402e, AFI 31-401 para 2.2.1.)			
1.1.2. Does the ISPM administer the program for all serviced activities, and fulfill assigned responsibilities? (AFI 31-401, para 1.3.4. & Chapter 2 & 5)			
1.1.3. Does the ISPM ensure derivative classifiers mark derivative classified documents properly? (para 3-102)			
1.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
1.2.1. Are decisions concerning declassification based on the 10 year rule. That is, unless exempted, is classified information automatically declassified 10 years after original classification? (para 4-201c)			
1.2.2. Are proper procedures followed with respect to requests for mandatory reviews of DoD classified information? (para 4-400)			
1.2.3. If classified documents being reviewed for declassification contain information that originally has been classified by another agency does the reviewing activity refer the appropriate portions to the originator authority? (para 4-401b)			
SECTION 2: SAFEKEEPING AND STORAGE			
2.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
2.1.1. If there is reasonable doubt about the level to classify information, is it safeguarded as appropriate pending a determination by an OCA or source document classifier? (para 3-201b)			

2.1.2. Is classified information or material stored in a locked security container, vault, room, or area according to its assigned classification level? (para 6-402)			
2.1.3. Are storage containers, vaults, and vault-type rooms protected by an alarm system or guarded during non-operating hours when they are located in buildings, structural enclosures, or other areas not under US Government control? (para 6-308 & Chapter 6 Section 4 & AFI 31-401 5.18.)			
2.1.4. Are combinations to security containers changed when required? (para 6-404b)			
2.1.5. Are combinations to security containers, vaults and secure rooms classified at the highest category of the classified information authorized to be stored therein? (para 6-404b(2))			
2.1.6. Are combinations limited to only those individuals who are authorized access to the classified information? (para 6-404b (4))			
2.1.7. Does the ISPM ensure repairs to damaged security containers are done according to proper procedures? (section 6-405 & AFI 31-401 5.24.)			
2.1.8. Are classified documents removed from storage kept under constant surveillance and covered by an appropriate classified cover sheet when not in storage? (para 6-301a & AFI 31-401 5.11.)			
2.1.9. Are preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, floppy disks, and typewriter ribbons adequately protected at the same level of information they contain? (para 6-301b & AFI 31-401 5.17.)			
2.1.10. Are plans developed for the emergency protection, removal, or destruction of classified material in detail commensurate with the assessment of risk? ***NOTE:*** Emergency destruction procedures are not required for units located in the 50 United States. (para 6-303 and AFI 31-401, para 5.6.)			
2.1.11. Does the ISPM ensure officials who arrange or convene a classified meeting or conference ensure the facility provides adequate security? (para 6-307 & AFI 31-401, para 5.15.)			
2.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
2.2.1. Does the ISPM ensure prohibited items, such as funds, weapons, medical security items, precious metals, or other items susceptible to theft, are not stored in security-type equipment (including vaults and vault-type rooms) used for storing classified material? (para 6-400)			
2.2.2. Has the ISPM ensured the installation commander provided a repository for in-transit/overnight storage of classified material? (AFI31-401, para 5.14.1.)			

2.2.3. Does the ISPM ensure Standard Form 700, **Security Container Information**, is properly maintained for each vault, secure room, or security container used for storing classified information? (para 6-404b(3) & AFI 31-401 5.23.2.)			
2.2.4. Does the ISPM ensure there are procedures established to prohibit the removal of Secret and Confidential classified material from an activity to do work at home, or for other reasons, unless approved by the head of a DoD component or their designee at the major command and higher levels, and then only when a GSA-approved security container is furnished to safeguard the material? (para 6-306 & AFI 31-401 5.13.)			
2.2.5. Does the ISPM ensure end-of-day security checks are being conducted and documented on Standard Form (SF) 701, "Activity Security Checklist"? (para 6-302 & AFI 31-401 5.12.)			
2.2.6. Does the ISPM ensure SF 702, **Security Container Check Sheet**, is used to record the use of all vaults, secure rooms and containers used for the storage of classified material? (para 6-302 & AFI 31-401 5.12.)			
SECTION 3: COMPROMISE OF CLASSIFIED INFORMATION			
3.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
3.1.1. Are security incidents promptly reported by personnel to either their security manager, immediate supervisor, commander, staff agency chief, or higher authority in the chain of command? (para 10-101b & AFI 31-401, para 9.2.1.)			
3.1.2. Does the ISPM ensure a preliminary inquiry is conducted to determine circumstances surrounding the security incident? (para 10-102a & AFI 31-401, para 9.6.)			
3.1.3. Does the ISPM ensure a formal investigation is conducted whenever the preliminary inquiry is insufficient to show results, or if otherwise required? (para 10-102b & AFI 31-401, para 9.3.)			
3.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
3.2.1. Does the ISPM ensure formal inquiry/investigation reports contain required information? (para 10-102)			
3.2.2. Does the ISPM follow-up to ensure the originator is notified and requested to conduct a review and reevaluation of the information subjected to compromise? (paras 10-103 and 10-104 & AFI 31-401 9.4./9.5.)			

3.2.3. Does the ISPM ensure formal investigation reports are reviewed and closed by an appointing authority? (AFI 31-401, para 9.4.)			
3.2.4. Does the ISPM ensure there are procedures in effect for conducting an inquiry when an individual having access to classified information is on unauthorized absence? ***NOTE:*** This requirement is based on the length of absence and degree of sensitivity of the classified information involved. (para 10-108 & AFI 41-401 9.7.)			
SECTION 4: ACCESS, DISSEMINATION, AND ACCOUNTABILITY			
4.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.1.1. Are personnel given access to classified information only if they have been determined trustworthy (a security clearance eligibility) and the access is necessary for performance of official duties (need-to-know)? (para 6-200 & AFI 31-401 5.4.)			
4.1.2. Does the ISPM ensure all Air Force cleared personnel (military and civilian) have signed the Nondisclosure Agreement? (para 1-101e & AFI 31-401, para 5.5.)			
4.1.3. Does the ISPM ensure procedures are followed for giving access to foreign nationals, foreign governments, international organizations, and immigrant aliens? (AFI 31-401 para 5.6.9.)			
4.1.4. Are Top Secret accountability registers (AF Form 143) maintained by each office originating or receiving Top Secret information, and do the registers reflect all required information? (AFI 31-401, para 5.10.1.1.)			
4.1.5. Do Top Secret Registers show current status and disposition of each Top Secret document? (AFI 31-401, para 5.10.1.1.)			
4.1.6. Does the ISPM ensure Top Secret documents and material are accounted for with a continuous chain of receipts? (AFI 31-401 para 5.10.1.2.1, 5.10.1.4.)			
4.1.7. Do unit commanders and staff agency chiefs develop and enforce procedures for control of Secret and Confidential material? (AFI 31-401 5.10.2.)			
4.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
4.2.1. Are procedures established to handle personnel who refuse to sign the SF 312, **Classified Information Nondisclosure Agreement**? (AFI 31-401, para 5.5.3.)			

4.2.2. Does the ISPM ensure unit commander or staff agency chief have designated a Top Secret Control Officer (TSCO), and alternates as necessary, to accomplish all matters affecting accountability and control of Top Secret material? (AFI 31-401 para 5.10.1.1.)			
4.2.3. Does the ISPM ensure AF Form 144 is kept with the document and destroyed two years after the document has been downgraded, declassified, or destroyed? ***NOTE:*** Do not remove the AF Form 144 when the document is transferred to another TSCA. (AFI 31-401, para 5.10.4. & AFMAN 37-139, table 31-4)			
4.2.4. Does the ISPM ensure Top Secret Register Pages are destroyed 5 years after page entries have been made inactive? (AFMAN 37-139, table 31-4)			
4.2.5. Does the ISPM ensure receipts and destruction certificates are retained for at least 2 years? (AFMAN 37-139, table 31-4)			
4.2.6. Do unit commanders and staff agency chiefs ensure an inventory is conducted at least annually or when there is a change in TSCO? (AFI 31-401, para 5.10.1.3.1.)			
4.2.7. Does the ISPM ensure classified working papers are properly marked and controlled? (para 6-101 & AFI 31-401 5.3.)			
4.2.8. Are there procedures established to ensure that equipment involved in reproducing classified material are properly posted with authority and clearances procedures? (AFI 31-401 para 5.17., 5.26., 5.27.)			
4.2.9. Does the ISPM ensure appropriate visual aids (AFVA 205-8 or AFVA 205-9 with AF Form 1112) are posted on or near equipment to denote authority or prohibition for using the equipment for classified reproduction? (AFI 37-162)			
4.2.10. Does the ISPM ensure copying of documents containing classified information is minimized? (para 6-502a)			
4.2.11. Does the ISPM ensure receipts are properly prepared, and is tracer action taken when signed receipts have not been returned by the imposed suspense date (30 days within CONUS, 45 days outside CONUS)? (AFI 31-401, para 6.6.4.1.)			
SECTION 5: TRANSMISSION			
5.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
5.1.1. Is classified information is transmitted only by approved methods? (Chapter 7 & AFI 31-401 Chapter 6 & AFI 31-401 8.8.2 & AFI 33-204)			
5.1.2 Does the ISPM ensure preparation of classified information for transmission, shipment, or conveyance meets minimum requirements? (para 7-200 & AFI 31-401 para 6.6.)			

5.1.3 Does the ISPM ensure proper procedures are followed when personnel escort or hand-carry classified material? (para 7-300b(2) & AFI 31-401, section 6c.)			
5.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
5.2.1. Does the ISPM ensure individuals who are authorized to hand-carry or escort classified material, receive an appropriate briefing, and are they required to acknowledge receipt of such briefing or instructions? (para 7-300b & AFI 31-401 6.7.)			
5.2.2. Does the ISPM ensure the restrictions and procedures governing the hand-carry of classified material aboard a commercial passenger aircraft properly adhered to? (para 7-302 & AFI 31-401, para 6.9.)			
5.2.3. Does the ISPM ensure that unit commander, staff agency chief, or security manager issue and control DD Form 2501, Courier Authorization or courier letter, for approving the hand carrying of classified material in the local area? (para 7-302b(2) & AFI 31-401, para 6.9.)			
5.2.4. If the base uses a pneumatic tube system to transmit classified material has it been approved by the Installation Commander? (para 7-100a & AFI 31-401, para 6.1.2.)			
SECTION 6: DISPOSAL AND DESTRUCTION			
6.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
6.1.1. Does the ISPM ensure only approved methods are used for destroying classified material? (6-701 & AFSSI 50-20 & AFI 31-401 5.29.)			
6.1.2. Does the ISPM ensure the proper type of equipment is available to adequately destroy classified material? (AFI31-401, para 5.29.1.)			
6.1.3. Does the ISPM ensure there are procedures instituted to ensure all classified information intended for destruction is actually destroyed? (para 6-700, 6-701)			
6.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
6.2.1. Are records of destruction are maintained for 2 years IAW AFMAN 37-139? (AFI 31-401, para 5.28.1.)			
6.2.2. Does the ISPM ensure procedures have been instituted that ensure all classified information intended for destruction is protected as appropriate? (para 6-700a)			

6.2.3. Does the ISPM ensure an annual clean-out day has been designated and procedures followed? (para 6-700b & AFI 31-401 5.28.3.)			
6.2.4. Are records of destruction attached the the AF Form 143, when the destruction is not recorded on the AF Form 143 itself? (AFI 31-401 5.29.2.1.3.)			
SECTION 7: SECURITY EDUCATION			
7.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
7.1.1. Are procedures followed when persons being debriefed refuse to sign the AF Form 2587? (10-105, AFI 31-401, para 8.11.)			
7.1.2. Does each military member and civilian employee receive initial orientation training upon reporting to each new unit? (9-200 & AFI 31-401, section 8b)			
7.1.3. Is it ensured that upon termination of employment, DoD military personnel and civilian employees are required to return all classified material and given a termination briefing, documented on AF Form 2587, **Security Termination Statement**? (para 9-500 & AFI 31-401 8.10.1.)			
7.2. NON CRITICAL ITEMS:	**YES**	**NO**	**N/A**
7.2.1. Does the ISPM ensure programs have been established to provide recurring security training for personnel having continued access to classified information? (para 9-400/401 & AFI 31-401, para 8.9.)			
7.2.2. Does the ISPM ensure personnel are informed of the techniques employed by foreign intelligence activities in attempting to obtain classified information, and their responsibility to report such attempts? (para 9-401)			
SECTION 8: FOREIGN GOVERNMENT INFORMATION			
8.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
8.1.1. Are procedures followed for the proper classification, declassification, and safeguarding of foreign government information? (para 6-600/2-501b/4-202)			
8.1.2. Are foreign government classified documents that do not have English language classification markings remarked with the US equivalent classification? (para 5-702)			
8.2. NON-CRITICAL ITEM:	**YES**	**NO**	**N/A**

8.2.1. Does the ISPM ensure DoD documents which contain NATO classified information are marked with the notation "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION"? (para 5-703c/d)			
SECTION 9: ADMINISTRATIVE SANCTIONS			
9.1. CRITICAL ITEMS:	**YES**	**NO**	**N/A**
9.1.1. Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent security violation occurs or repeated administrative discrepancies or repeated disregard of the requirements of DoD 5200.1-R occur? (para 1-501 & 31-401 1.8.1.)			
9.1.2. Are original classification authorities (OCA) indoctrinated in the fundamentals of security classification, limitations on their authority to classify information, and their responsibilities as such prior to the exercise of this authority? (para 2-200/9-300/9-301 & AFI 31-401 Chapter 2)			
9.1.3. When unusual compilation circumstances occur. Is classification by compilation of unclassified items of information, fully supported by written explanation that is required to be provided with the material so classified? (para 2-400 & 5-206c)			
9.1.4. Are classification guides which are not listed in DoD 5200.1-I and do not require an executed DD Form 2024 because of the classification considerations, reported separately to the Director of Security Plans and Programs, OASD (CI & SCM)(C3I)? (para 2-502e)			
9.1.5. Does the ISPM ensure originators review classification guides for currency and accuracy at least once every 5 years, and if no changes are made, is the record copy annotated to show the date of the review? (para 2-503a)			
9.1.6. Does the originator of each guide execute DD Form 2024, **DoD Security Classification Guide Data Elements**, when the guide is approved, changed, revised, reissued, or canceled, and when its biennial review is accomplished? (para 2-503a, 503d)			
SECTION 10: PROGRAM MANAGEMENT			
10.1. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
10.1.1. Does the ISPM ensure unit commanders or staff agency chiefs have appointed a security manager, and necessary alternates, to make sure the information security program is implemented in the activity? (AFI 31-401, para 1.3.5.)			
10.1.2. Does the ISPM ensure the SM has received proper training to perform the job? (para 9-303 and AFI 31-401, para 1.3.4.)			

10.1.3. Does the ISPM ensure the unit commander or staff agency chief has designated personnel to conduct semiannual security inspections of the activity? Are the inspections sufficient in scope to identify and correct problems? (AFI 31-401, para 1.4.4.)			
10.1.4. Does the ISPM ensure the activity is collecting and reporting data on the SF 311, "**Agency Information Security Program Data**," to satisfy the report requirements of the Information Security Oversight Office (ISOO)? (para 1-600a and AFI 31-401, para 1.7.)			
10.1.5. Does the ISPM ensure if holders of classified information have reason to believe that information is classified improperly or unnecessarily, do they communicate that belief to their security manager or the classifier of the information to bring about a review of the material? (para 4-900)			
10.1.6. Does the ISPM ensure challenges to the classification of Air Force information is sent through ISPM channels to the originator? ***NOTE:*** Challenges to the classification of non Air Force information are sent to HQ USAF/SFI for resolution? (para 4-900 & AFI 31-401, para 2.3.)			
SECTION 11: MARKING			
11.1. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
11.1.1. Does the recipient contact the originator in all cases when classified material is received with improper markings? (para 5-102a)			
11.1.2. Does the ISPM ensure the original classification authority responsible for classification of the information is identified on the "classified-by" line? (para 5-202a)			
11.1.3. Does the ISPM ensure when "multiple sources" is listed on the "classified-by" line, that these sources are identified and maintained with the file/record copy of the document? (para 5-202b(2))			
11.1.4. Does the ISPM ensure major components of complex documents, i.e., annexes and appendices, are properly marked? (para 5-300)			
11.1.5. Does the ISPM ensure documents are properly marked? (para 5-102, 5-206a, 5-207a, 5-300, 5-301, 5-Section 4)			
11.1.6. Does the ISPM ensure transmittal documents are properly marked? (Section 5-301)			